REMARKS/ARGUMENTS

Reconsideration of this application is requested. Claim 1 has been amended herein to clarify the scrambling function recited in step (d). No new matter has been introduced by this amendment.

In the Official Action, the Examiner has rejected claims 1-6, 8-9 and 13-14 under 35 USC 102(e) as being anticipated by Vancelette (U.S. Pat. 5,893,320). This rejection is traversed, as the cited reference fails to disclose, teach or suggest each of the limitations recited in present claim 1.

Independent claim 1 recites:

> A method for managing access to a scrambled event from a service provider, said method comprising:
> (a) receiving in a device associated with the user an electronic list of events, at least one event having an encrypted message associated therewith;
> (b) receiving in said device, in response to user selection of said event, said encrypted message;
> (c) decrypting said encrypted message to obtain a descrambling key;
> (d) receiving said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event; and
> (e) descrambling said selected event using said descrambling key.

In complete contrast, Vancelette discloses a method for enabling a user to select how he or she wishes to view a given event, after already receiving and processing the event data stream. Vancelette fails to disclose or suggest all of the method steps (a)-(e) recited above in claim 1, and clearly does not teach or suggest "receiving said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to

said selected event" where the "descrambling key" was previously obtained by decrypting an encrypted message that was received in response to user selection of a given event from a list of events received at the device (emphasis added).

More particularly, the Vancelette reference discloses a number of video and/or audio data packets corresponding to various camera/audio feeds that cover a particular event. Control messages from an operator interface are combined with the packetized data to form a packetized data stream (see col. 6, lines 24-26). The packetized data stream is then encrypted "in accordance with one or more cryptographic keys to prevent unauthorized viewers from accessing the programming" (see column 6, lines 57-60). The encrypted, packetized data stream is then transmitted to a set top terminal device 70, where it is received and decrypted (see module 530 of FIG. 5). The "decrypted" (i.e. "unscrambled" or "clear") audio/video packets are then separated from the "decrypted" (i.e. "unscrambled" or "clear") control information, and processed separately (see modules 540, 555 of FIG. 5). A Microprocessor 540 then determines which of the "clear" video/audio packets within the decrypted packet stream are to be processed and displayed to the user based on the control information and certain user selections. However, it is abundantly evident that, at this point, all of the audio/video data contained within the set top device is "in the clear" and available for viewing. The "clear" control information is simply used by the set top terminal to now select a certain, already decrypted or descrambled channel of audio/video packets from a number of available channels for viewing by the user. The "selected event" of Vancelette is thus in no way "scrambled using said descrambling key (column 6, lines 25-35) where the descrambling key is the object code which

provides the alternatives related to the audio and video capabilities (column 9 lines 15-22)" as proposed by Examiner on page 1 of the present office action. Clearly, the control information is not at all used in Vancelette to "scramble" the selected event, and is certainly not used for "preventing unauthorized access to said selected event" as recited in step (d) of present claim 1.

Rather, the invention recited in present claim 1 requires that the selected event or program, when received at the receiving device, be scrambled or encrypted using the descrambling key previously obtained in step c) of claim 1, so as to prevent unauthorized access to the selected event. In Vancelette, the particular "event" to be displayed (i.e. the particular video/audio feed) is only selected after the data packets for various channels (i.e. various "events" comprising multiple video/audio feeds) have already been descrambled/decrypted and available at the set top box by means of a decrypting/descrambling key (col. 6, lines 56-58 and col. 9 lines 4-6). Accordingly, Vancelette does not and cannot teach or suggest each of the limitations recited in method claim 1. For at least these reasons, claim 1 is patentable in a '102 sense over Vancelette. Reconsideration and removal of this rejection is respectfully urged.

Claims 7, 10-12 and 15-20 stand rejected under 35 USC 103(a) as being unpatentable over Vancelette and further in view of Pinder et al (US Patent 6,105,134). The arguments discussed hereinabove with regard to patentability of claim 1 apply as well to these claims, including independent claims 15 and 18. Moreover, Pinder does nothing to overcome the deficiencies associated with Vancelette discussed above. Independent claim 15 recites additional features and limitations, including

> "receiving an electronic program guide from a guide provider, said guide having a message and a digital signature associated with each event in said guide, said message being encrypted using a public key of the smart card and said digital signature being created using a private key of said guide provider" (emphasis added).

The Examiner states that:

> "Pinder discloses the use of the private key used for digital signatures" and that it would have been obvious "to use the private key for a digital signature created using a private key as in Pinder in the system of Vancelette...because the digital signature operations provide authentication." (Pinder col. 5 lines 34-35).

While Pinder indeed discloses the use of digital signatures in a cable TV system, no where is any suggestion or motivation to be found in either of the cited references, nor in science and logic, to somehow utilize the digital signature disclosed in Pinder in any manner within the mutli-channel, viewer selectable, video/audio system of Vancelette in an attempt to arrive at applicant's claimed invention. Such a combination is merely a piece-meal selection of individual elements from Pinder and Vancelette, which combination is not supported by the teachings of any of these references. Moreover, present claims 15 and 18 recite further additional features, including the use of a "symmetric key" for scrambling/descrambling, and of a "first public key" and "second private key" for performing the authentication prior to descrambling of the actual event or program received at the device. For at least these reasons, present claims 15 and 18 are patentable in a '103 sense and should be allowed.

In view of the foregoing, Applicants respectfully submit that claims 1-20 are in condition for allowance. Favorable reconsideration is therefore respectfully requested.

If a telephone conference would be of assistance in advancing prosecution of the above-identified application, Applicants' undersigned Attorney invites the Examiner to telephone him at **609-734-6815**.

Respectfully Submitted

Date: 11-26-03

42,670

Paul Kiel
Registration No. 40,677

THOMSON LICENSING INC.
Patent Operations
CN 5312
Princeton, NJ 08543-0028